

FIGURE 1A

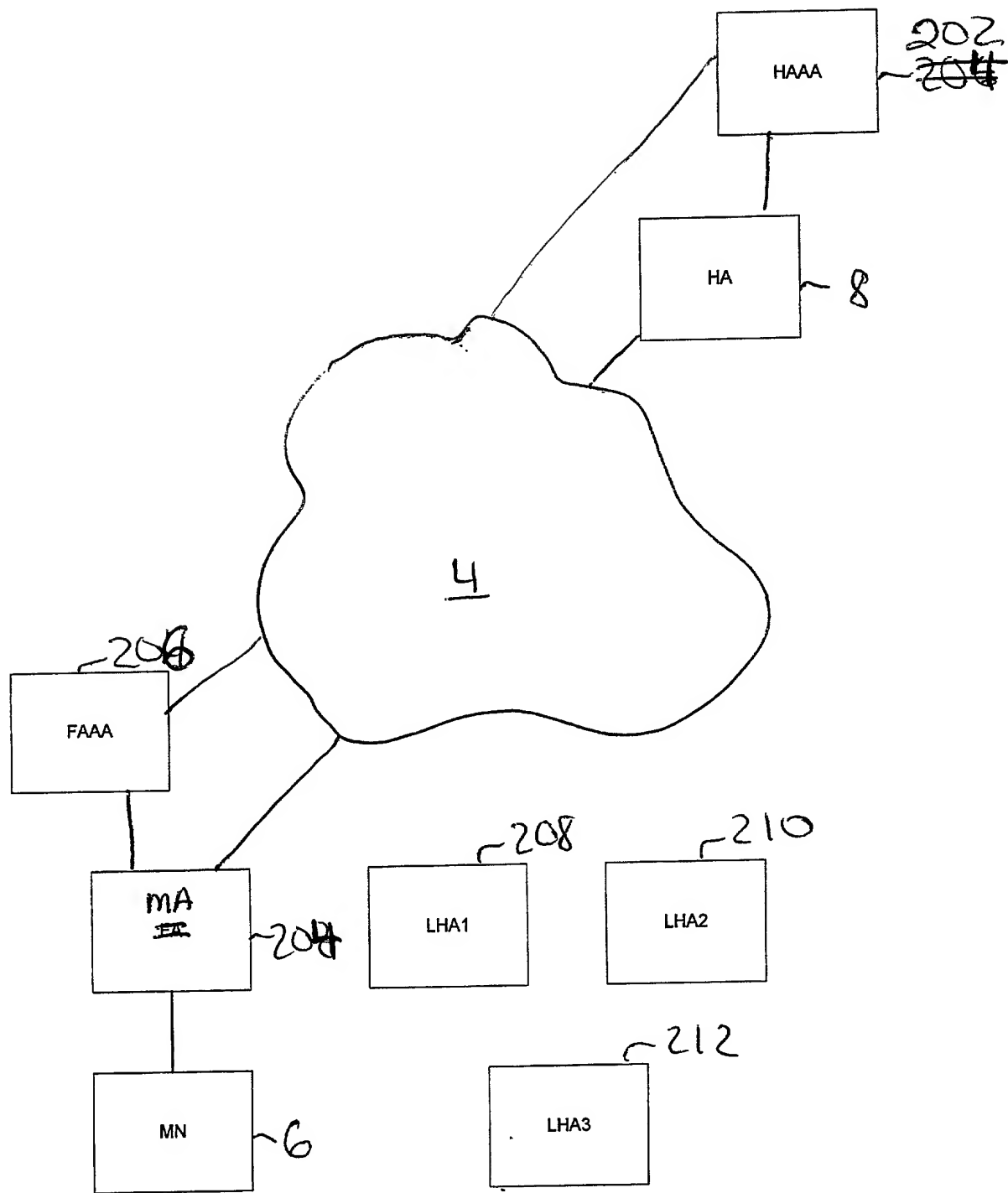
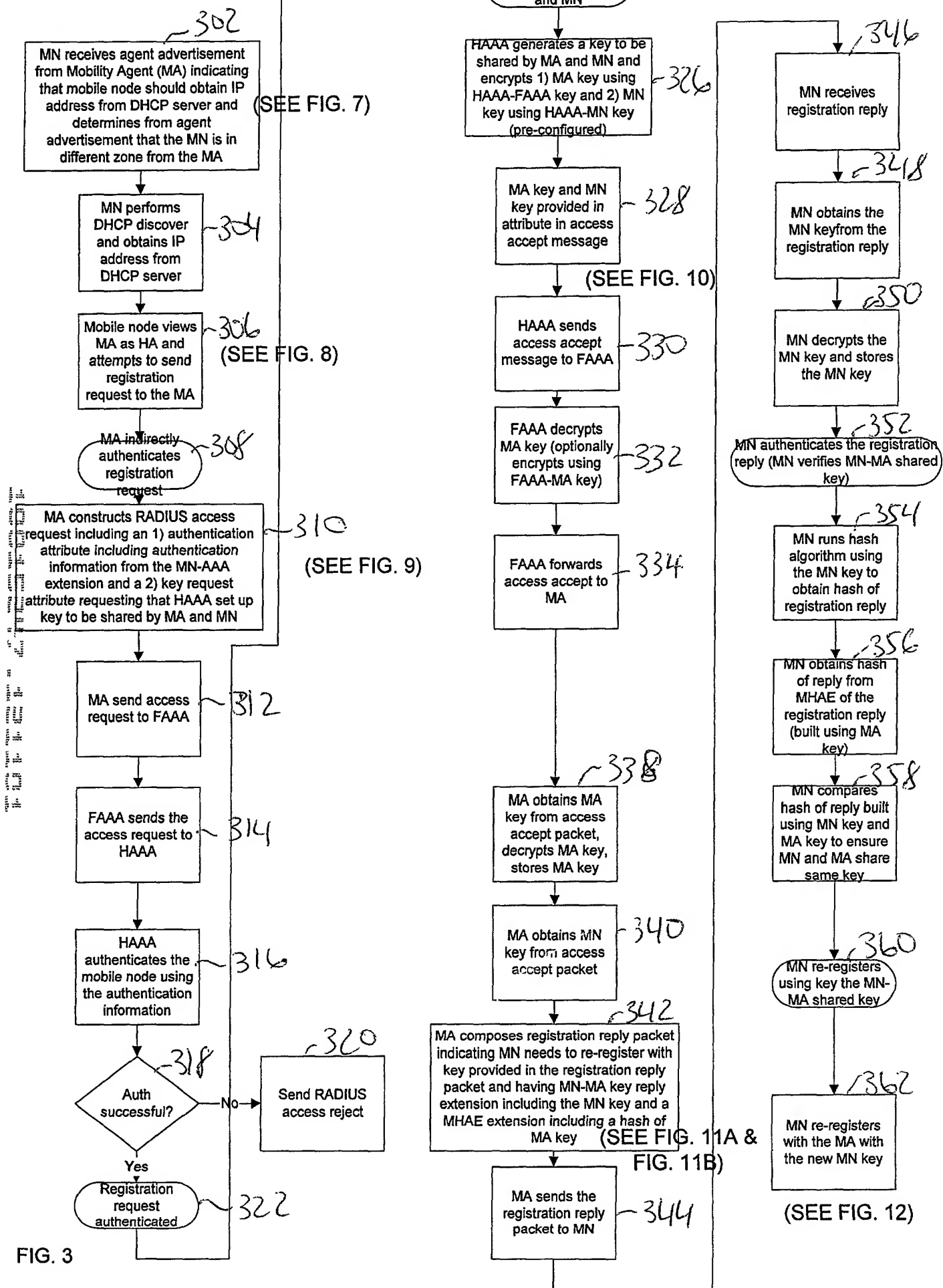
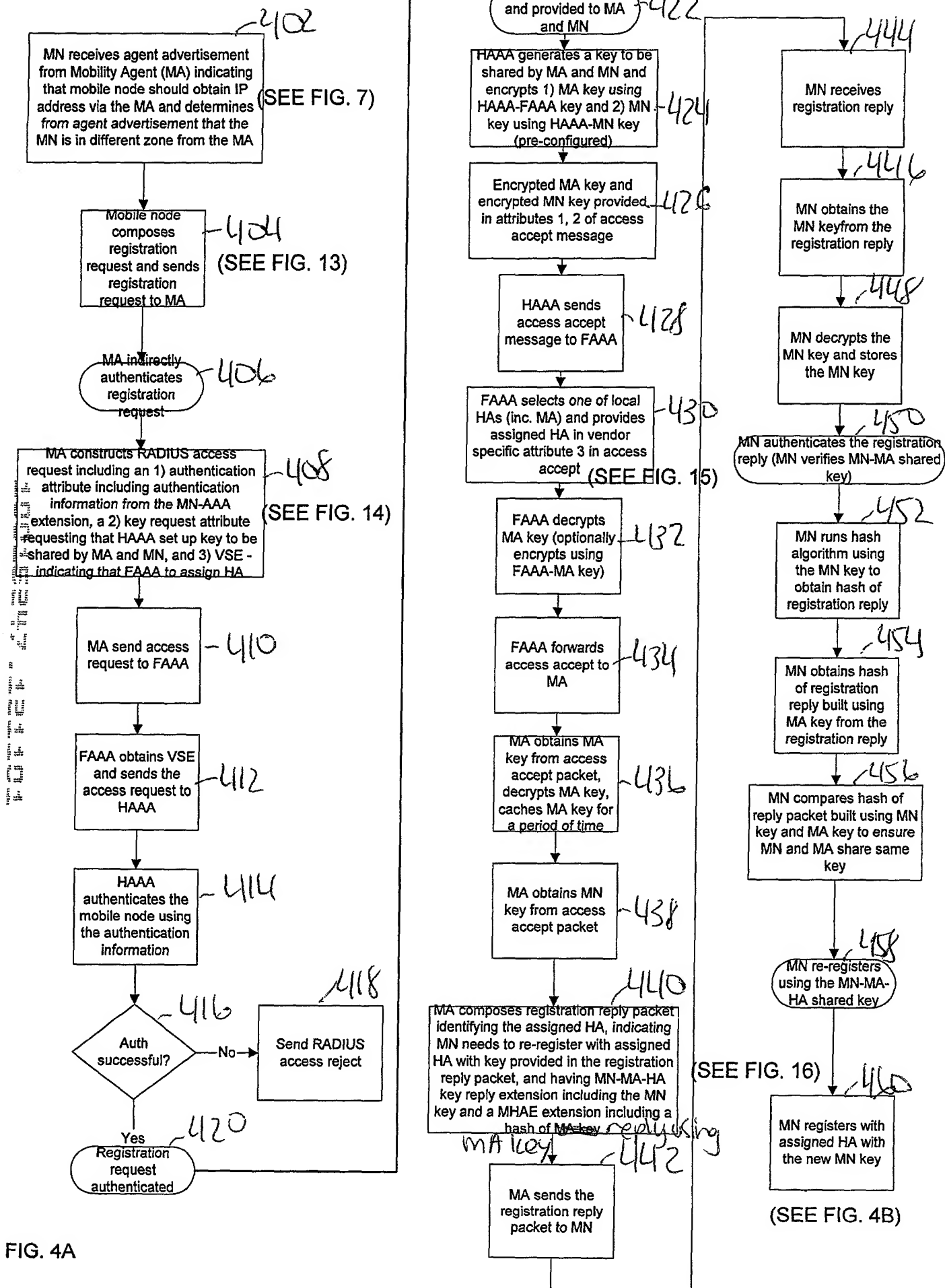


FIG. 2





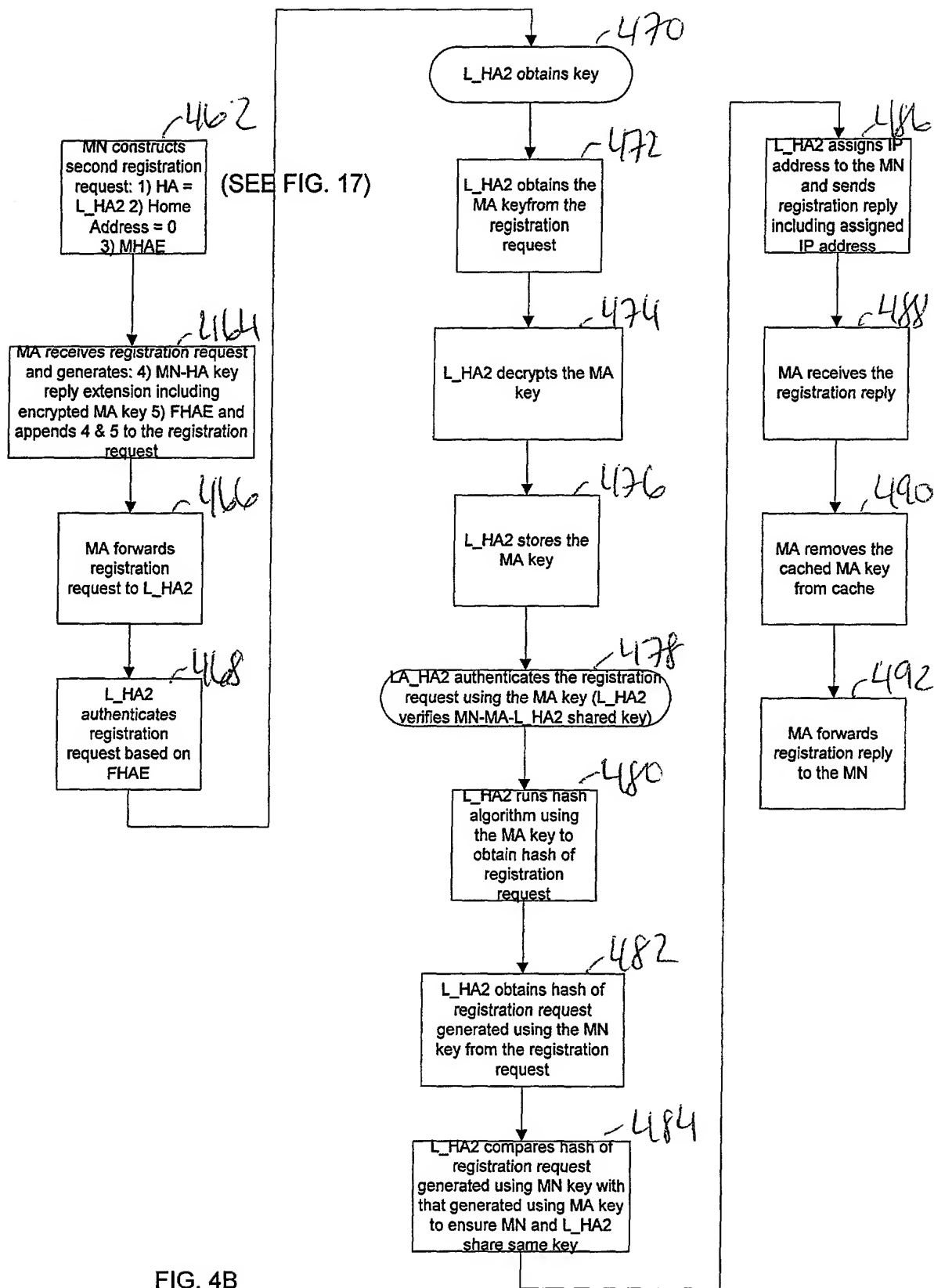
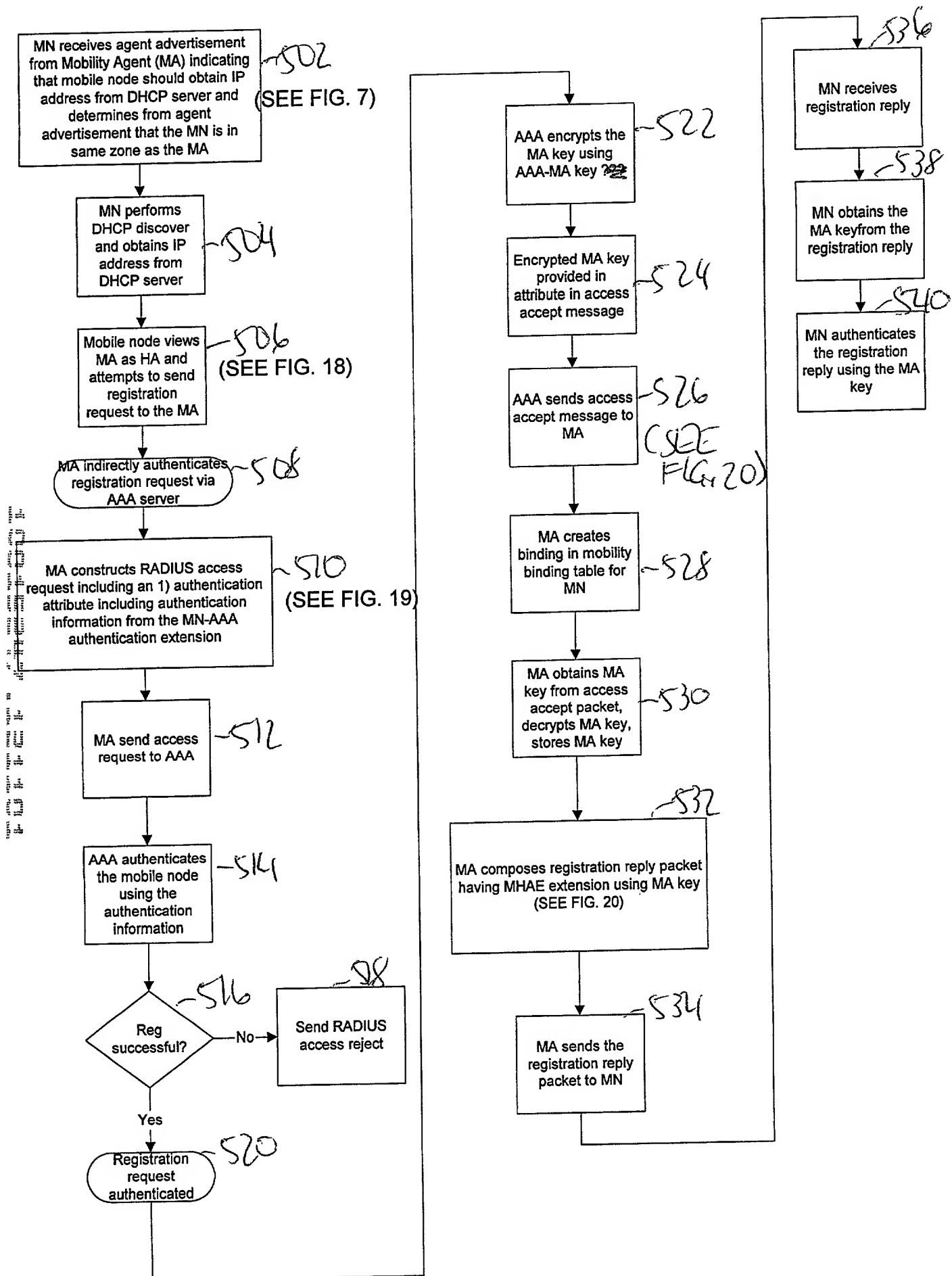


FIG. 4B



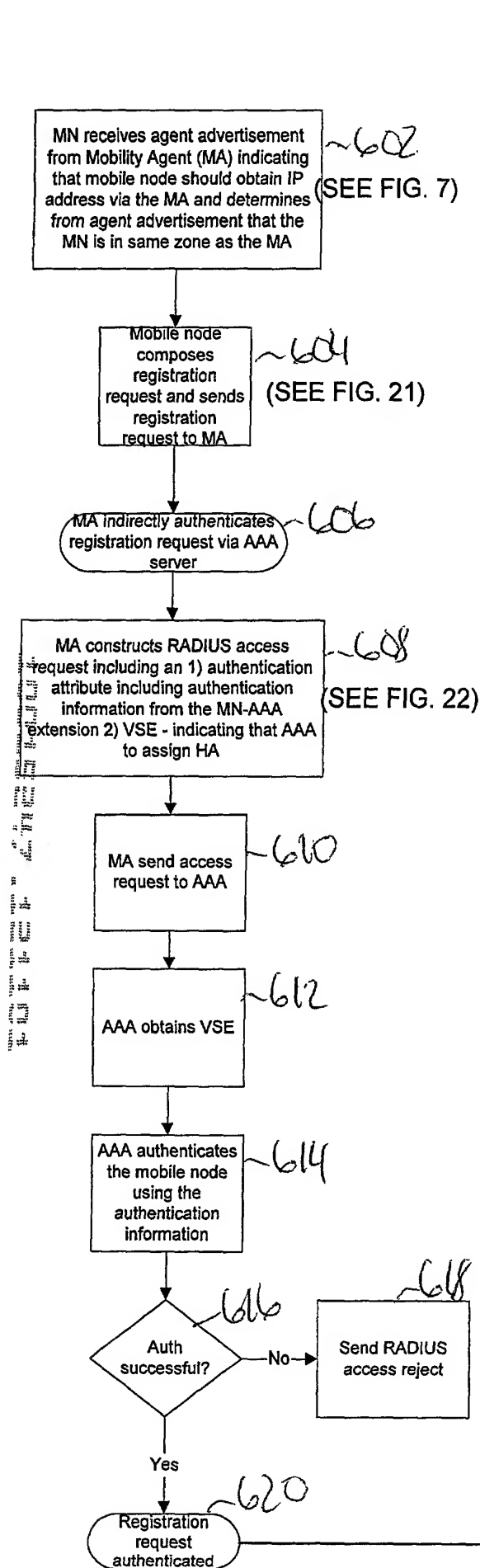
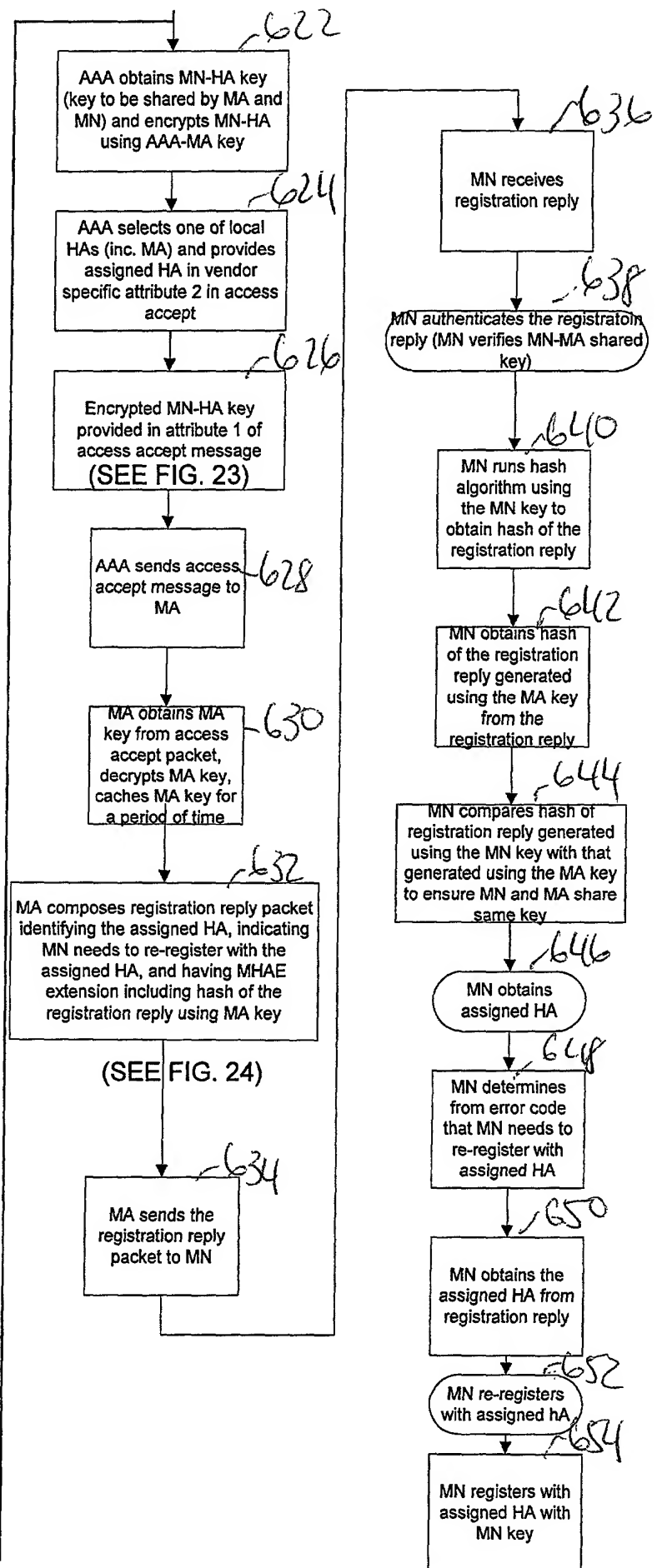


FIG. 6A



(SEE FIG. 6B)

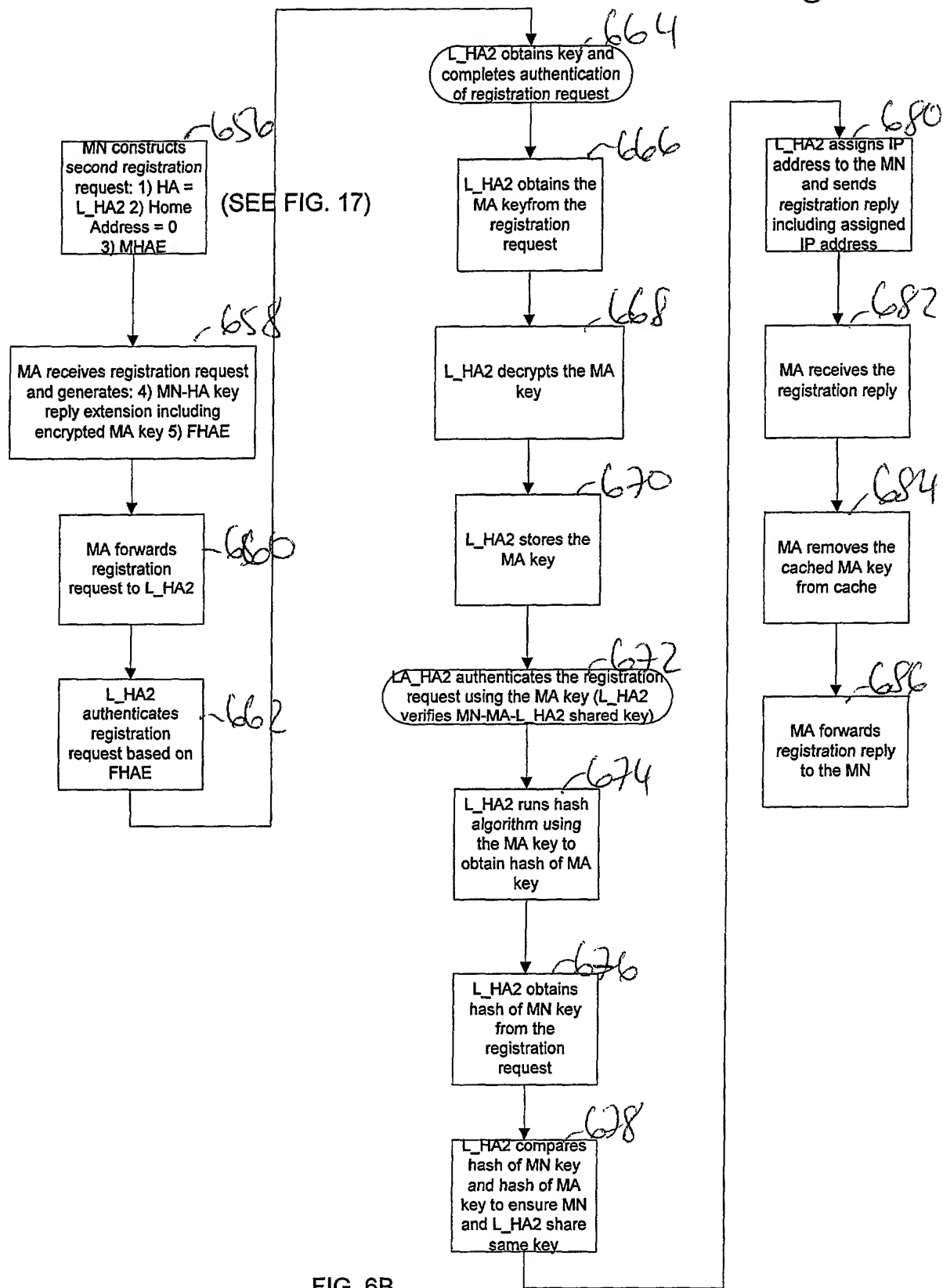


FIG. 6B

Mobility Agent Advertisement

702 Agent advertisement - providing mobility services (e.g., H and F bit set)	704 Extension 1: Zone	706 Extension 2: Obtain IP address from DHCP server (or MA)
--	--------------------------	--

FIG. 7

Registration request

802 Registration request: 1) Home Address = DHCP address 2) Home Agent address = MA address	803 NAI Extension	804 MN-MA key request extension indicating to HAAA to set up key to be shared by MA and MN (used to authenticate MA and MN)	806 MN-AAA authentication extension including hash value of registration request using shared key between MN and HAAA
--	----------------------	--	--

FIG. 8

Access request

902 Access request:	904 Key request attribute indicating to HAAA to set up key to be shared by MA and MN (used to authenticate MA and MN)	906 Authentication attribute including hash value generated using shared key between MN and HAAA
------------------------	--	---

FIG. 9

Access accept

1002 Access accept	1004 MA key	1006 MN key
-----------------------	----------------	----------------

FIG. 10

FIG. 11A is a block diagram of a registration reply message structure. The message structure includes a registration reply field, a vendor specific extension field, a key reply extension field, and an MHAE field. The registration reply field includes an error code (e.g., 0 indicating registration successful, new key error code indicating that the mobile node needs to obtain MN key and re-register with the MN key). The vendor specific extension field indicates that the mobile node needs to obtain MN key to authenticate message and re-register with the MN key. The key reply extension field includes the MN key. The MHAE field includes a hash of the reply using the MA key.

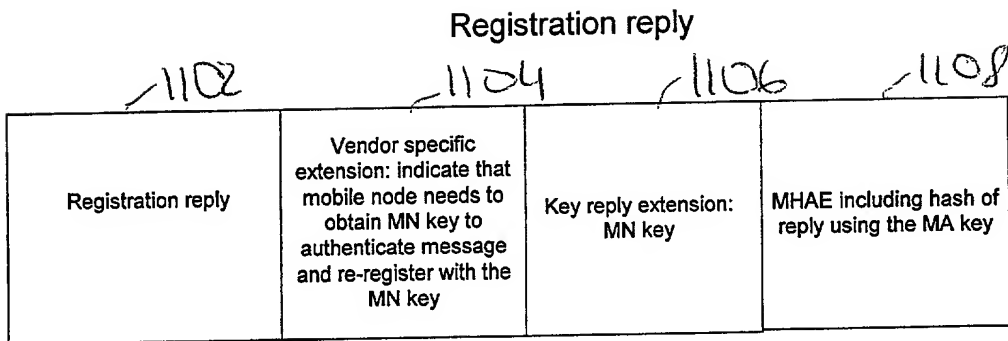


FIG. 11A

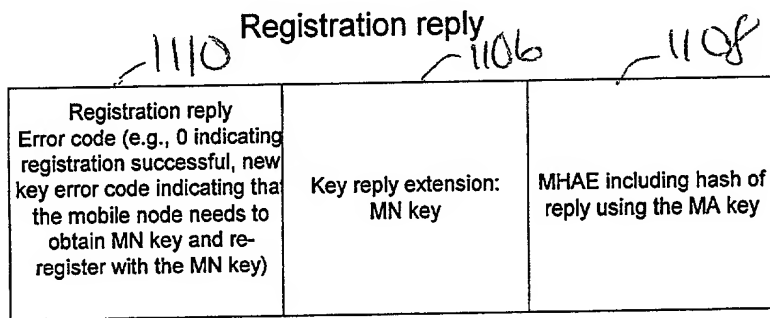


FIG. 11B

Registration request

1202 803 1204

Registration request: 1) Home Address = DHCP address 2) Home Agent address = MA address	NAI Extension	MHAE authentication extension including hash value generated using the MN key shared by the MN and the MA
---	---------------	---

FIG. 12

Registration request

1802	1308	1304	1306
<p>Registration request:</p> <p>1) Home Address = 0</p> <p>2) Home Agent address = 0 indicating load balancing desired</p>	<p>NAI extension including mobile node identifier</p>	<p>MN-MA key request extension indicating to HAAA to set up key to be shared by MA and MN (used to authenticate MA and MN)</p>	<p>MN-AAA authentication extension including hash value generated using shared key between MN and HAAA</p>

FIG. 13

Access request

¹⁴⁰²	¹⁴⁰⁴	¹⁴⁰⁶	¹⁴⁰⁸
Access request:	Key request attribute indicating to HAAA to set up key to be shared by MA and MN (used to authenticate MA and MN)	Authentication attribute including hash value generated using shared key between MN and HAAA	Vendor specific attribute indicating FAAA to assign HA

FIG. 14

Access accept

¹⁵⁰²	¹⁵⁰⁴	¹⁵⁰⁶	¹⁵⁰⁸
Access accept	MA key	MN key	Assigned HA (e.g., L-HA2)

FIG. 15

Registration reply

1602	1604	1606	1608
Registration reply - HA = assigned HA (e.g., L_HA2)	Key reply extension: MN key	Vendor specific extension: indicate that mobile node needs to obtain MN key to authenticate message and re-register with the assigned HA with the MN key	MHAE including hash of registration reply generated using MA key

FIG. 16

1610
Registration reply Error code (e.g., 0 indicating registration successful, new key error code indicating that the mobile node needs to obtain MN key and re-register with the MN key)

Registration request

1702	1704	1706	1708
Registration request: 1) Home Address = 0 2) Home Agent address = assigned HA (e.g., L_HA2)	MHAE authentication extension including hash value of reply generated using the MN key shared by the MN and the MA	MN-HA key reply extension including encrypted MA key	FHAE (e.g., MA-L_HA2)

FIG. 17

Registration request

<p>1802</p> <p>Registration request: 1) Home Address = DHCP address 2) Home Agent address = MA address</p>	<p>1804</p> <p>MN-AAA authentication extension including hash value generated using shared key (MA key) between MN and AAA</p>
--	--

FIG. 18

Access request

<p>1902</p> <p>Access request:</p>	<p>1904</p> <p>MN-AAA attribute including hash value generated using shared key (MA key) between MN and AAA</p>
------------------------------------	---

FIG. 19

Access accept

<p>2002</p> <p>Access accept</p>	<p>2004</p> <p>MH-AE: Encrypted MA key</p>
----------------------------------	--

FIG. 20

Registration request

<i>-2102</i>	<i>-2106</i>	<i>-2104</i>
Registration request: 1) Home Address = 0 2) Home Agent address = 0 indicating load balancing desired	NAI extension including mobile node identifier	MN-AAA authentication extension including hash value generated using the shared key between MN and AAA

FIG. 21

FIG. 22 is a diagram illustrating an access request message structure. The message is divided into three fields: an access request field (2202), an MN-AAA attribute field (2204) including a hash value for a shared key (MA key/MN-HA key) between MN and AAA, and a vendor specific extension field (2206) indicating FAAA to assign HA.

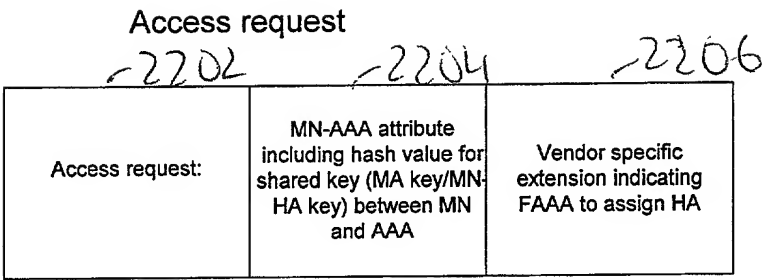


FIG. 22

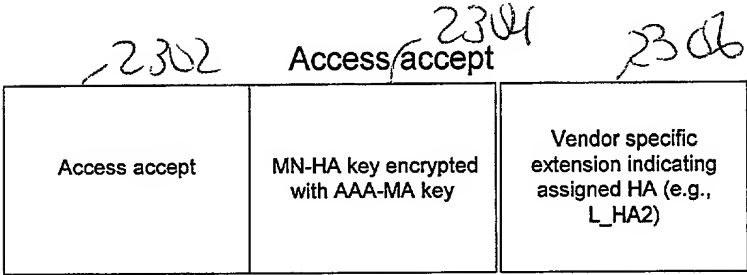


FIG. 23

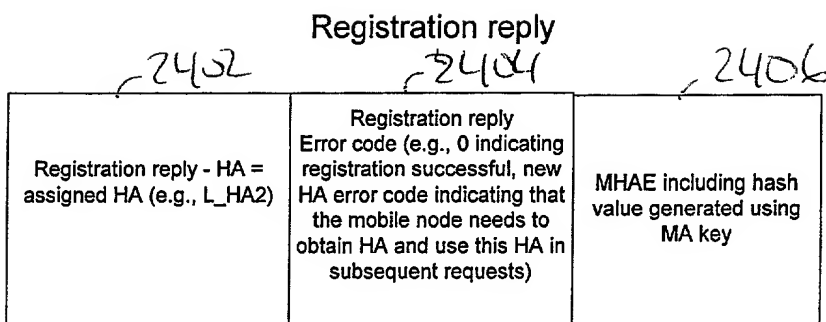


FIG. 24

